System Security Officer (SSO) Checklist:

Tasks that SSOs Need to Complete

Initial Security Requirements:

1. Designate a system security officer (SSO) in writing (use the template letter provided). (30 minutes to 1 hour)
   http://fsanet/cio/products/it_security_portal/personnel/sso_assignment_letter_template.doc

2. Designate a system manager in writing . (30 minutes to 1 hour)

3. Complete an inventory worksheet and submit to FSA Computer Security Officer staff. (2 to 4 hours)
   http://fsanet/cio/products/it_security_portal/inventory_worksheet/blank_inventory_worksheet.doc

4. Complete a CIP survey and submit to FSA Computer Security Officer staff. (2 to 6 hours)
   http://fsanet/cio/products/it_security_portal/forms/critical_infrastructure_protection_program_survey_cipp2003.xls

5. Determine if you need to complete a Privacy impact assessment (PIA), and, if yes, complete the PIA
   http://fsanet/cio/products/it_security_portal/privacy/privacy_impact_assessment_template_july2003.doc

6. System will be assigned a tier level (from the FSA Computer Security Officer).

WAIT UNTIL YOU RECEIVE A SYSTEM TIER LEVEL FROM THE FSA CSO

7. Complete a system security plan (use the provided template)
   http://fsanet/cio/products/it_security_portal/system_security_plan/index.html

8. Complete a configuration management plan (use the provided template)
   http://fsanet/cio/products/it_security_portal/config_management/index.html

9. Complete the appropriate contingency plans (either a continuity of support plan, a disaster recovery plan, or both; use the provided “contingency plan” template for a continuity of support)
   http://fsanet/cio/products/it_security_portal/cont_support/index.html

10. Have an independent risk assessment conducted
    http://fsanet/cio/products/it_security_portal/risk_assessment/index.html

11. Create a corrective action plan to remediate risk assessment security findings.

12. Ensure that all contractors accessing the system have undergone the appropriate background checks.
    http://fsanet/cio/products/it_security_portal/personnel/guide_to_clearance_paperwork.doc

13. Become familiar with the system life cycle (SLC)
    http://fsanet/cio/products/it_security_portal/slc/index.html

14. Have the contingency plan/disaster recover procedures tested

15. Put system through Certification and Accreditation (C&A)
    http://fsanet/cio/products/it_security_portal/c_and_a/index.html

16. Respond to C&A findings

Ongoing Security Requirements

- Update inventory worksheet (twice a year)
- Complete NIST 800-26 self-assessment (annually)
- Update CIP survey (annually)
- User account management (adding/deleting/modifying)
- Processing new system users (background checks, etc.)
- Respond to audit findings (periodically, at least annually)
- Recertify systems (every 3 years, or if system undergoes a major change)
- Attend SSO meetings (8 times/year)

Useful Resource:

- The Online Security Center: Go to FSAnet, then click on the “Tech Center” tab at the top, then click on “Online Security Center”—all the guidance, templates, etc., you need are located there. In particular, read the FSA System Security Process Guide (located under the Policies/Regulations > FSA Policies).